“White Collar” Theft Prevention

William P. McManus
Chief of Police

210-224-STOP
Crime Stoppers of San Antonio works in partnership with citizens, media, and law enforcement to reduce and prevent crime in the San Antonio area.

You can report crime and Wanted Felons by calling
210-224-STOP (7867)

All calls are completely confidential and all callers remain anonymous. If your information leads to the arrest or filing of charges on a felon, you will receive a cash reward up to $5000!

The following tips provide ways to reduce the chances of you and your business from becoming the victim of a white collar theft, such as embezzlement or credit card fraud.

GET YOUR OWN MAIL

- The MOST effective step in reducing your chances of becoming an embezzlement or "Employee Theft" victim is to GET YOUR OWN MAIL; every day. Have a CLEAR and WRITTEN policy, signed by each employee, as to where the mail should be stored or placed, if delivered in your absence.

- Stop the mail if going out of town for more than 1 or 2 days. Helpful Hint: Get to know your mail carrier. They can be very helpful and understanding of your wishes on how you wish to "receive" the mail.

DELEGATE TASKS

- A common error, especially in small businesses, is to have the same person handle the following tasks: accepting sales transactions, paying bills & invoices, making bank deposits, and reconciling bank/credit card accounts. These tasks should be handled by, minimally, two different people. Try and switch the tasks around, between individuals, periodically.

- Be aware of the bookkeeper that makes themselves appear to be absolutely indispensable. You should never rely too heavily on any one bookkeeper or accountant. Sometimes the person taking company funds is your most tenured, loyal, and hardworking employee.

HANDLING DAILY BANK DEPOSITS

- Make all deposits yourself. But if you are not able to, verify each deposit before it is sent to the bank.

- Review the deposit slip upon its return to the office.

- Reconcile bank statements within 5 days of receipt. Be sure all deposits match and don't forget to verify the "deposit dates" as well. Question anything that does not "look right."

ISSUANCE OF BUSINESS CHECKS FOR DAILY OPERATIONS

- Never sign a blank check. **EVER.**
- Keep blank checks in a locked cabinet. Have a key policy signed by anyone that has a key that accesses the check storage location.
- When possible review your canceled checks for any suspicious transactions or checks that the payees do not match with your check register.
- ELIMINATE ALL SIGNATURE STAMPS. Never give the power of your signature to anyone else. If you must have one though keep it locked in a secure area and limit access to only yourself.

BUSINESS BANK STATEMENTS

- For extra security, have bank statements sent to your home. Bring copies of ALL bank statements home. Make this known to your bookkeeper/accounting staff.
- Be sure to reconcile all statements within 5 days of receipt. Question everything that does not look right.
- Obtain all credit reports for yourself, business partners, and the business every six months, but minimally once a year. Be sure to receive credit reports from ALL three of the following: Experian, Equifax, and Trans Union. Contrary to popular belief, credit reporting firms DO NOT share information.

  Experian 1-888-397-3724 or www.experian.com
  Trans Union 1-800-680-7289 or www.transunion.com
  Equifax 1-800-525-6285 or www.equifax.com

- Incorporate a credit monitoring service. Strongly encourage all employees to do the same.
- Check on-line bank statements on a daily basis. Question anything that does not make sense.
- Do not feel awkward if your bank statement is confusing. Many bank statements are/can be confusing, be sure to meet with your bank representative to have them answer any and all questions you may have. The bank will hold you accountable for not understanding how to read and understand your bank statements. Be sure you clearly understand how to read all of your statements.

DAILY RECONCILIATION OF CASH TRANSACTIONS

- Daily cash sales should be reconciled each day. If you are not able, have at least two individuals, sign off on the cash sales report or ledger.

- Have at least one individual independently review/verify the cash deposit and have them sign off on the amount.

- If your company does not handle "cash sales" on a routine or daily basis, be sure all cash customers are provided with a receipt stating the amount of the transaction and the initials of the employee who received the cash.
- Have a written (and signed by all employees) policy as to where all cash is to be stored, before being deposited into the bank.

- If you have a "petty cash" on hand, routinely verify the receipts against the cash remaining. Essentially, reconcile the petty cash monthly.

- ALL receipts must be originals and signed or initialed by the individual reimbursed by or using the petty cash account.

- Be sure petty cash is locked in a secured area. Have a written key policy that is signed by everyone who received a key to the petty cash storage location.

MONTHLY INVENTORIES

- Inventories should be completed monthly and yearly.

- Suspicious overages or shortages should be reviewed immediately.

- Have a requisition system to note when merchandise is received or shipped from your company.

VERIFY VENDOR INVOICES

- Routinely check vendor invoices to ensure the vendor payments and credits associated with the vendor are reasonable and accurate.

- Verify all vendor invoices and be sure the vendor payment matches the invoiced amount.

- Question multiple checks written to anyone particular vendor, especially if you do not recognize them.

- If you do not recognize the vendor, CALL them yourself. Ask questions.

COMPANY CREDIT CARDS

- Have a written policy that is signed by all employees with credit card privileges. Be very specific on how all company credit cards must be used and how their use will be tracked.

- Reconcile all credit card statements within 5 days of receipt. Know that you lose many rights to dispute charges after 30 days of a statement date.

- Be sure ALL receipts turned in by employees are originals NOT copies.

- Personally shred all "retired" credit cards with a "D.O.D. (Department of Defense) approved" shredder. A shredder that meets D.O.D. standards cross cuts items into very small pieces.

- Personally shred ALL credit card offers you have no intention of accepting, upon receipt. Do not file these offers for later use. Use them or personally shred them, with a D.O.D. approved shredder.

WHEN CLOSING A BUSINESS CREDIT CARD ACCOUNT…….

- Personally shred all unwanted credit cards with a "D.O.D. (Department of Defense) approved" shredder. A shredder that meets D.O.D. standards cross cuts items into very small pieces.

- If you no longer wish the credit card or account to be used, clearly tell the credit company you want to "Hard Close the Account" NOT just "close the account".

- If you expect a zero balance on a closed credit card account, be sure you receive, review and file the statement showing a zero balance.

IF YOUR COMPANY ACCEPTS CREDIT CARDS…….

- It is critical to review the daily batch reports - *daily.*

- Be on the look out for multiple "refunds" in even or round numbers such as $15.00, $52.00, $125.00, $500.00, etc. Typically an employee that is "misapplying your company funds" will often forget to add cents to the "fraudulent refund amount" and most legitimate transactions will have some pennies/cents in the transaction amount. Multiple even dollar refund amounts should be considered SUSPICIOUS.

- Watch for "repeated refunds" to the same credit card number.

BUSINESS COMPUTER USAGE

- Check sent in inbound emails for anything suspicious. Make it known to all employees the business computers are YOUR COMPUTERS NOT THEIRS, and that you may periodically review the contents of their work or emails.

AUDITS

- Randomly audit the company's books; minimally twice a year. Be sure these surprise audits are just that, a surprise.

PAYROLL SERVICE

- Fraud & theft through payroll accounts is common. Employing a payroll service will virtually eliminate the opportunity for fraud through the payroll accounts

LOANS TO EMPLOYEES

- The best option is to not loan money to employees. But if you do, have clear-written terms that are signed by you and the employee. Clearly state the loan amount and the payback terms including time line, especially if you will be deducting the payback from the employees check.

DISHONEST EMPLOYEE INSURANCE COVERAGE

- Ask your business insurance carrier about "Dishonest Employee Insurance." It is very cost-effective and wise to have this additional coverage.

FINANCIAL POINTS OF CONTACT

- Be sure you are very clear with the banks and lending institutions as to who is your company's "Financial Point of Contact." Be sure "Financial Points of Contact" are primary partners in the firm. Keep "Financial Points of Contact" to a strict minimum. Should the bank need to speak with your bookkeeper, be clear with the bank they are authorized to speak with said individual on a call-by-call basis. As soon as that specific call has ended, the bank must again ask for permission to speak with said individual, even for follow-up questions on the same question or topic.

SAN ANTONIO POLICE DEPARTMENT CONTACTS

For information on the Internet: **http://www.sanantonio.gov/SAPD/**

Property Crimes is now located at the substation in you area:

Substation	Address	Property Crimes #
SOUTH	**711 W.Mayfield**	**207-7184**
EAST	**3635 E.Houston**	**207-8854**
CENTRAL	**515 S.Frio**	**207-7990**
NORTH	**13030 Jones Maltsberger**	**207-7601**
WEST	**7000 Culebra**	**207-8299**
PRUE	**5020 Prue Rd.**	**207-8326**

FINANCIAL CRIMES UNIT

The SAPD Financial Crimes Unit has case management responsibilities for embezzlement, official integrity, and major fraud cases. Details within the Financial Crimes Unit include FORGERY, and WHITE COLLAR CRIMES.

WHITE COLLAR CRIME DETAIL:

The White Collar Crime Detail has investigative and case management responsibilities for all embezzlement, integrity and major fraud cases. WHITE COLLAR CRIMES can be reached at 207-4481.

FORGERY DETAIL

The Forgery Detail has investigative and case management responsibilities for all check forgeries, credit card abuse, and counterfeit offenses. FORGERY can be reached at 207-7451.